2021-06-24 Minutes

Attendees:

Voting Participants: Ken Dagg, Martin Smith, Richard Wilsher, Mark Hapner, Mark King

Non-voting participants: Jimmy Jung, , Pradheep Sampath, , Roger Quint, Eric Thompson

Invited Guests: Jeremy Haynes, Blake Hall, Rohan Pinto, Pete Eskew

Staff: Kay Chopard, Ruth Puente

Agenda:

1. Administration:
    a. Roll Call
    b. Agenda Confirmation
    c. Minute approval (DRAFT minutes of 2021-06-03)
    d. Staff reports and updates
    e. LC reports and updates
    f. Call for Tweet-worthy items to feed (@KantaraNews)
2. Discussion
    a. Consideration of 'comparable alternatives' - See: https://groups.google.com/g/idassurance/c/GlGLjVaIdg4
    b. Australian Digital Identity Legislation Consultation Phase 2 - See: Public consultation on Australia's Digital Identity legislation
    c. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. See: https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation
    d. d. Component Service Consumer criteria.

Meeting notes:

<u>Administrative items:</u>

IAWG Chair Ken Dagg called the meeting to order at 1:05PM (US Eastern), and called the roll. It was noted that the meeting was quorate.

Agenda confirmation: Ken noted that the order of Discussion items had been changed from the original meeting announcement to accommodate the "comparable alternatives" item that is believed to be of current interest to CSPs.

Chair comments: Ken welcomed the new Kantara Executive Director (ED), Kay Chopard, and invited her to introduce herself. Kay said she is very impressed with the variety of important work being done in Kantara and specifically in the IAWG, citing today's full agenda as an example. She has so far been fully occupied with learning how Kantara operates and meeting people in Kantara and from other organizations interested in working with us, but she looks forward to contributing to the substantive work very soon. She called out particularly the assistance Ruth Puente has been providing to support a quick and smooth transition. She invited meeting participants to reach out to her at kay@kantarainitiative.org.

Ken noted that Ruth is also transitioning to a new position at another organization as of July 1. He congratulated her but also expressed how important she has been to maturing Kantara's Assurance Program during her 7 years and a half association with us. He also thanked her for her excellent support of the IAWG. Richard Wilsher added that she has been a "great accomplice." Kay commented that finding a new Assurance Program Manager is one of her highest priorities, and that she is currently evaluating several candidates.

Ken added that pending a new APM getting up to speed, the WG will be on its own for administrative support and is in need of a volunteer Secretary to prepare Minutes. He emphasized that responsibility does not require a great deal of time and invited IAWG participants to contact him if they might be able to step up.

Minutes approval: Mark Hapner moved approval of the the draft Minutes of the IAWG meeting of June 3; Eric Thompson seconded. The Minutes were approved unanimously, as written.

Staff reports and updates: Ruth Puente reported that the assessment program is quite active and she anticipates approval of 4 new Service Providers over the next months.

LC reports and updates: Ken said the LC has approved a very substantive report on mDL Privacy prepared by the Privacy and Identity Protection in mobile Driving License ecosystems DG (PImDL DG), which is now in the publication pipeline. He believes the report will be very influential because it documents a number of significant privacy issues that mDL solutions will have to address.

Ken reminded WG participants that Kantara staff is ready to help them publicize their newsworthy activities and via the @KantaraNews Twitter handle.

Discussion:

Consideration of 'comparable alternatives' - See: https://groups.google.com/g/idassurance/c/GlGLjVaIdg4

Ken asked Richard Wilsher to introduce the topic and provide background.

Background: It was commented that there is a US Federal Agency that is interested to know if Kantara has an opinion or guidance related to NIST 800-63-3, 5.4 - Risk Acceptance and Compensating Controls. In this section, the guidance states that the "Agencies MAY determine alternatives to the NIST-recommended guidance, for the assessed xALs, based on their mission, risk tolerance, existing business processes, special considerations for certain populations, availability of data that provides similar mitigations to those described in this suite, or due to other capabilities that are unique to the agency." It follows that agencies "SHALL demonstrate comparability of any chosen alternative, to include any compensating controls, when the complete set of applicable SP 800-63 requirements is not implemented." (pp 22-23). The agency is specifically concerned about the disparate impact on digital ID proofing for a relatively low inherent fraud risk within their program. They have risk assessed that this falls into IAL2, but think it is a candidate for this 'comparable alternative" ID Proofing. However, there is no guidance on how to demonstrate comparability or details related to appropriate justification.

Moreover, this Agency is interested to explore the feasibility of a third party framework to certify Comparable Alternatives as allowed for in section 5.4 of NIST 800-63-3, such as Kantara.

Richard said Sec 5.4. does allow US Federal agencies to use "comparable alternatives" and provides some guidance on how that would be done. Richard suggested that KI might perform an assessment of a service that used an alternative control, but he feels that Kantara can't take on determination of what is "comparable."

Richard shared draft language for an approach to this issue Kantara might take:

I suggest that the best way for Kantara to address this is to introduce a new criterion which states:
If a CSP implements alternative controls for any specific proofing requirements for the applicable xAL, the CSP SHALL ensure that:
  a) a quantitative analysis of the risk(s) addressed by the NIST-specified control and the degree of residual risk its implementation would achieve is determined and documented;
  b) a justification of how the compensating measures deployed achieve equivalent or comparable mitigation of the same risks is determined and documented;
  c) a justification of how different risks that may be introduced through the use of the alternative controls have been taken into account such that the same, or lower, residual risk can be achieved is determined and documented;
  d) that the responsible management are aware of and accepting of that analysis and the implementation of the selected controls;
  e) that the selected counter-measures are deployed;
  f) how to configure the service to provide a risk mitigation level commensurate with the consumer's own risk mitigation needs is documented and provided to users who wish to rely upon the service at the claimed xAL.

Richard further reported discussion of this issue with David Temoshok of NIST. He said David discouraged KI involvement in assessing these alternative controls because it's the Federal Agencies CIO responsibility; he further believes use of such alternatives would only be appropriate to address a use-case unique to one agency.

Blake Hall said he believe the "Federal agency" Richard mentioned is the Department of Labor, which is exploring the possibility of allowing the use of expired drivers licenses as identity documentation for their public "customers." Blake said his company hopes to service this requirement.

Eric Thompson agrees that there should be alternatives for the large number of people who lack the currently acceptable identity documents.

Martin Smith suggested that from what has been said, it sounds like this issue could best be addressed via the upcoming revision of SP-800-63-A that could provide for more flexible (and thus more inclusive) identity-proofing alternatives. But of course 800-63 Rev. 4 will not be promulgated some time next year.

Roger Quint said the question is: what are we trying to accomplish? Are we developing a general strategy for addressing special cases? He said Kantara should avoid getting in the middle of hard determinations.

Ken summarized the situation by saying it appears there are two distinct issues: a gaping hole in 800-63-3, and how Kantara might deal with the "comparable alternative" process..

Chairman Dagg called time on the discussion as 2:59PM. He characterized the discussion as very useful and said Kantara will need to settle on an approach soon. He confirmed that the WG will meet next week to continue this discussion and, if possible, address other issues on today's Agenda that were not discussed.

Next Meeting: Next Thursday, July 8 at 1PM US Eastern (July 1st is a national holiday in Canada)